UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA - against - NARAY PALANIAPPAN, Defendant.	**15-CR-485 (FB)**

MOTION TO SUPPRESS EVIDENCE

Law Office of Zachary Margulis-Ohnuma
260 Madison Avenue, 17th Fl.
New York, NY
(212) 685-0999
zach@zmolaw.com

Attorneys for Defendant Naray Palaniappan

Table of Contents

FACTS 2
ARGUMENT 4
I. The NIT search of Mr. Palaniappan's computer required a warrant. 5
II. The NIT Warrant was invalid because it was issued in violation of the plain language of Rule 41 7
A. Rule 41(b) does not authorize a warrant seeking information outside the district in these circumstances. 7
B. The warrant did not and could not authorize the NIT to be installed as a tracking device. 11
III. Suppression of evidence gathered as a result of the intrusion into Mr. Palaniappan's computer is warranted. 14
A. The NIT warrant was void ab initio and therefore its fruits should be suppressed. 15
B. Under Second Circuit law, where a federal warrant is signed by a judge not authorized by Rule 41(b), the violation is constitutional and suppression is appropriate. 16
C. Suppression is warranted here because Mr. Palaniappan was prejudiced and the government willfully disregarded Rule 41. 18
1. Prejudice 18
2. "Intentional and Deliberate Disregard of the Rule" 22
D. Suppression is appropriate in this case to deter law enforcement overreaching 23
CONCLUSION 24

Defendant Naray Palaniappan hereby moves pursuant to Rule 12(b)(3)(c) of the Federal Rules of Criminal Procedure to suppress all evidence obtained from the government's illegal search of his computer through the use of a "Network Investigative Technique" (NIT) in violation of the Fourth Amendment of the United States Constitution, 28 U.S.C. § 636(a), and Fed. R. Crim. P. 41. This includes all evidence, including computers, electronic media, and digital images, collected from Mr. Palaniappan during the illegal search in February 2015 and during a subsequent search of his home on September 1, 2015 that was authorized by an Eastern District of New York warrant based on evidence collected from the prior illegal search.

In brief, the initial search of Mr. Palaniappan's computer violated Rule 41 and the U.S. Constitution because it purported to be supported by a warrant that was plainly invalid under Rule 41's geographical limitations as they existed at that time. Fed. R. Civ. P. 41(b)(1) - (4) (2015 ed.) (limiting search warrant to a magistrate judge with authority in the district where the search takes place). Moreover, agents executing the February 2015 search willfully flouted both Rule 41 and the specific language of the warrant by failing to notify Mr. Palaniappan he had been surreptitiously searched until more than a year after the search was executed. Under these unusual circumstances, the evidentiary fruits of the search of the personal computer should be suppressed to vindicate the prejudice to Mr. Palaniappan and to deter future violations of the law by FBI agents.[1]

FACTS

On September 1, 2015, eight armed agents from the Federal Bureau of Investigation ("FBI") raided the Queens apartment of Naray and Kavitha Palaniappan and their two children, who were four and two years old at the time. The agents spent approximately four hours at the apartment, much of it rummaging through the family's bedroom and the apartment's closets. They entered and searched the home pursuant to a search warrant issued by Magistrate Judge Marilyn Go of the Eastern District of New York. *See* Ex. A (warrant). The warrant was based on an affidavit submitted by FBI Special Agent John Vourderis. Ex. B (Vourderis Affidavit). Mr. Palaniappan was arrested later that day after the administration of a polygraph examination at FBI headquarters in Manhattan.

According to the Vourderis Affidavit, the Palaniappan home was identified as part of "Operation Pacifier," the investigation into users of the Playpen child pornography website operated by the FBI from February 20 to March 4, 2015. *See* Dkt. No. 30 at 2-4: Palaniappan Motion to Dismiss (describing government's

[1] In the event the evidence is not suppressed based on this basis, we respectfully request that the Court hold a hearing pursuant to *Franks v. Delaware* to determine whether the agent signing the warrant misrepresented the probable cause supporting the warrant to the issuing magistrate. In particular, we respectfully submit that there is evidence that the FBI knew or should have known that the Playpen's homepage no longer displayed child pornography at the time the NIT warrant was issued and failed to convey that fact Magistrate Judge Buchanan in seeking the NIT warrant. In the event the evidence is not suppressed for the reasons stated herein, we respectfully request an opportunity to fully brief and present evidence regarding these misrepresentations and the need for a *Franks* hearing.

operation of child pornography website); *see also* Ex. B: Vourderis Aff. ¶ 23 (describing operation of the NIT), ¶¶ 26-27 (acknowledging use of NIT to obtain IP address). Specifically, the FBI conducted another, earlier search of Mr. Palaniappan's computer, presumably on or about February 25, 2015, when the IP address for the username "JIMINYCRACKET" was discovered. *Id.* ¶ 26 ("According to data obtained from logs on Website A, monitoring by law enforcement, and the deployment of a NIT, on February 25, 2015, the user 'JIMINYCRACKET' engaged in the following activity on Website A from IP address 66.65.172.171."). That IP address was associated with Mr. Palaniappan's apartment in Queens, New York. The user JIMINYCRACKET, according to data obtained from the website itself, "accessed" child pornography. *Id.* ¶ 27. But in order to discover the IP address and other identifying information for JIMINYCRACKET, the FBI had to break the defenses of the remote computer—which turned out to be Mr. Palaniappan's—and infect it with coded instructions that would transmit the identifying information back to a government computer.[2] *See* Ex. E (warrant application for NIT) ¶ 33.

That search purported to be authorized by a warrant issued not in the Eastern District of New York, but by the Hon. Theresa Carroll Buchanan, a federal

[2] In other contexts, such instructions would be referred to as executable malware, like that used by thieves to commit blackmail or steal banking information. *See, e.g.,* Poulsen, Visit the Wrong Website and the FBI could End Up on Your Computer, *Wired*, *available at* www.wired.com/2014/08/operation_torpedo/ ("From the perspective of experts in computer security and privacy, the NIT is malware, pure and simple."). We call it the NIT here because that is the preferred nomenclature of its creator, the government, but we respectfully submit that the term is a misleading euphemism.

magistrate judge in the Eastern District of Virginia. *See* Ex. C (the so-called "NIT warrant"). It was based on an affidavit executed by FBI agent Douglas McFarlane. Ex. D. The warrant specifically directed agents to notify Mr. Palaniappan within 30 days of the search. Ex. C at 1. However, he was not notified or provided a copy of the warrant until a year later, when the NIT warrant was disclosed in discovery in the criminal case. *See* Ex. F (Palaniappan Affidavit).[3]

ARGUMENT

The initial search in this case was plainly illegal under the Fourth Amendment because it was not authorized by a valid warrant and no exception to the warrant requirement applies. U.S. Const. Amend. IV. The "warrant" signed in the Eastern District of Virginia was not capable of authorizing the search of Mr. Palaniappan's computer in Queens because the judge who signed it did not have jurisdiction to authorize a search in Queens under Rule 41 as it existed at the time. *See* Fed. R. Crim. P. 41(b)(2).[4] This error was a "fundamental" violation of the rule because, in effect, no warrant existed at all. *See U.S. v. Williamson*, 439 F.3d 1125,

---

[3] In an email received today, AUSA Tanya Hajjar asserted that "the government obtained extensions of delayed notice of the NIT warrant and your client was timely notified." I have requested but not yet received these notices, which should have been turned over pursuant to Rule 16. Their existence and contents admittedly could change the analysis of whether the government deliberately violated Rule 16.

[4] Effective yesterday, Rule 41 was amended at the request of the Department of Justice to accommodate out-of-district warrants such as this. However, references herein are to the version of Rule 41 in effect at the time of the search of Mr. Palaniappan's computer unless otherwise noted. The rule change is further evidence that the government was fully aware that the warrant was not valid under the old version of the rule in effect at the time of the search. *See* http://www.uscourts.gov/rules-policies/current-rules-practice-procedure, *last accessed* Dec. 2, 2016 (official court website listing rule changes going into effect on December 1, 2016, including new Fed. R. Civ. P. 41(b)(6) which provides for out-of-district warrants to seize electronic information in circumstances similar to those here).

1132-33 (9th Cir. 2008) (Rule 41 violation that renders a search unconstitutional is "funadamental" and warrants suppression). It was of constitutional magnitude because the user of the computer had a reasonable expectation that information stored on the computer, which revealed intimate details of the user's internet activity, would remain private. Even if the Rule 41 violations were merely technical, though, suppression would be appropriate because Mr. Palaniappan was prejudiced by it in the sense that, if the rules had been followed—*i.e.* if the scope of the warrant were limited to the Eastern District of Virginia or if Mr. Palaniappan had been properly notified—the incriminating evidence would never have been discovered by law enforcement. Accordingly, all evidence arising from the NIT search of Mr. Palaniappan's computer, including his subsequent statements and evidence seized from his home, should be suppressed.

I. THE NIT SEARCH OF MR. PALANIAPPAN'S COMPUTER REQUIRED A WARRANT.

As a preliminary matter, the execution of the NIT on Mr. Palaniappan's computer was a "search" for purposes of the Fourth Amendment—which is, of course, why the government sought the warrant in the first place. *See U.S. v. Ammons*, No. 3:16-CR-00011-TBR-DW, 2016 WL 4926438 at *4 (W.D. Ky. Sept. 14, 2016) ("There appears to be no dispute that [the Defendant] enjoyed a subjective expectation of privacy in the contents of his personal computer. His expectation was reasonable too."); *U.S. v. Darby*, No. 2:16CR36, 2016 WL 3189703 at *5 (E.D. Va. June 3, 2016) (The NIT was a search because it "surreptitiously placed code on Defendant's personal computer that then extracted from the computer certain information.").

Individuals typically possess a reasonable expectation of privacy in information stored on their home computers. *U.S. v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004); *see also U.S. v. Ganias*, 755 F.3d 125, 135 (2d Cir. 2014), *reh'g en banc granted,* 791 F.3d 290 (2d Cir. 2015) ("Like 18th Century "papers," computer files may contain intimate details regarding an individual's thoughts, beliefs, and lifestyle, and they should be similarly guarded against unwarranted Government intrusion."). The warrant purported to authorize the search and seizure of detailed personal information connecting users to the Playpen website, specifically including the IP address, the type of operating system running on the target computer, the computer's host name, the username used to login to the computer, and the computer's media access control address ("MAC address"). *See* Ex. C: NIT Warrant, attachments B (listing information to be seized). But the entire contents of the computer, including these items, are protected by the Fourth Amendment. *See Riley v. California*, 134 S. Ct. 2473, 2492 (2014) (extracting even call logs from a cell phone constitutes a search).

Searches performed without "prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." *Katz v. United States*, 389 U.S. 347 (1967). None of the legally recognized exceptions to the warrant requirement applies here, and thus the government was required to obtain a valid warrant from an authorized magistrate judge before searching Mr. Palaniappan's computer.

II. THE NIT WARRANT WAS INVALID BECAUSE IT WAS ISSUED IN VIOLATION OF THE PLAIN LANGUAGE OF RULE 41

Rule 41(b) carefully describes the geographical jurisdiction of magistrate judges to issue warrants. Fed. R. Crim. P. 41. In Subsection (A), *infra*, we demonstrate that nothing in the rule permits a magistrate judge in the Eastern District of Virginia to authorize a search in New York, unless it is for property that was in Virginia at the time the warrant issued or related to terrorism. *Id*. In Subsection (B), *infra*, we address the small number of cases that have erroneously found that the Virginia had authority based on the "tracking device" provision of Rule 41(b)(4).

A. Rule 41(b) does not authorize a warrant seeking information outside the district in these circumstances.

The search of Defendant's home and computer systems on September 1, 2015 was the direct result of an earlier illegal search of his computer made possible by the use of the NIT malware. The warrant authorizing the deployment of the NIT malware against Defendant's computer, located in New York, was issued by a magistrate judge located in the Eastern District of Virginia. The territorial limitations on a magistrate's authority under Rule 41(b), however, clearly prohibit the issuance of such a warrant. Specifically, Rule 41(b) limits a magistrate's ability to issue warrants to the following five circumstances:

> **(b) Authority to Issue a Warrant.** At the request of a federal law enforcement officer or an attorney for the government:
>
> > **(1)** a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property *located within the district;*
> >
> > **(2)** a magistrate judge with authority in the district has authority to issue a warrant for a person or property *outside the district if the person or property is located within the district when the warrant is issued* but might move or be moved outside the district before the warrant is executed;
> >
> > **(3)** a magistrate judge—in an investigation of *domestic terrorism or international terrorism*—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;
> >
> > **(4)** a magistrate judge with authority in the district has authority to issue a warrant to install within the district *a tracking device*; the warrant may authorize use of the device to track the movement

> of a person or property located within the district, outside the district, or both; and
>
> **(5)** a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but *within any of the following*:
>
>> **(A)** a United States territory, possession, or commonwealth;
>>
>> **(B)** the premises--no matter who owns them--of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or
>>
>> **(C)** a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

Fed. R. Crim. P. 41(b) (emphasis added).

None of these provisions applies on its face to a situation where a Virginia magistrate judge authorized FBI agents to search a computer located in Queens. The NIT warrant is therefore is plainly unlawful. A clear majority of district courts have found that, under Rule 41, the NIT warrant *could not* authorize searches of computers outside of the Eastern District of Virginia. *See U.S. v. Levin*, -- F.Supp.3d --, No. CR 15-10271-WGY, 2016 WL 2596010 at *5 (D. Mass. May 5, 2016) ("[b]ecause the NIT warrant purported to authorize a search of property located outside the Eastern District of Virginia, and because none of the exceptions to the general territorial limitation of Rule 41(b)(1) applie[d], . . . the magistrate judge lacked authority under Rule 41(b) to issue the NIT Warrant"); *U.S. v. Michaud*, No. 3:15-CR-05351-RJB, 2016 WL 337263 at *6 (W.D. Wash. Jan. 28, 2016) (Rule 41"does not directly address the kind of situation that the NIT warrant was authorized to investigate, namely, where criminal suspects' geographical whereabouts are unknown, perhaps by design, but the criminal suspects had made contact via technology with the FBI in a known location"); *U.S. v. Henderson*, No. 15-CR-00565-WHO-1, 2016 WL 4549108 at *4 (N.D. Cal. Sept. 1, 2016) (holding that "[t]he NIT Warrant was invalid under Rule 41(b) because the NIT search was not permissible under any of the five subsections of the Rule"); *U.S. v. Ammons*, No. 3:16-CR-00011-TBR-DW, 2016 WL 4926438 at *6 (W.D. Ky. Sept. 14, 2016) ("Because [the] Magistrate Judge . . . had no jurisdiction or authority under [Rule 41(b)] to issue the NIT warrant, . . . the NIT warrant was void from the beginning[.]"); *U.S. v. Ryan Anthony Adams*, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at *6 (M.D. Fla. Aug. 10, 2016)(The "subsections of Rule 41(b) relied upon by the Government clearly render a warrant authorizing a search outside of the issuing magistrate judge's district ineffective[.]"); *U.S. v. Werdene*, No. CR 15-434, 2016 WL 3002376 at *7 (E.D. Pa. May 18, 2016) (Because "the computer information that the NIT targeted was at all relevant times located beyond the boundaries of the Eastern District of Virginia . . . [t]he magistrate judge was . . . without authority to issue the NIT warrant under Rule 41[.]"); *U.S. v. Anzalone*, No. CR 15-10347-PBS, 2016 WL 5339723 at *9 (D. Mass. Sept. 22, 2016); *U.S. v. Workman*, No. 15-CV-00397-RBJ-1, 2016 WL 5791209 at *4 (D. Colo. Sept. 6, 2016) (holding that "[a] plain reading of the current Rule 41(b) and proposed Section (6) indicates that Section (6) is an entirely new grant of magistrate judge authority," referring to the amendment that took effect yesterday); *U.S. v. Allain*, No. 15-CR-10251, 2016 WL 5660452 at *11 (D. Mass. Sept. 29, 2016) (finding that no section of Rule 41(b) is applicable); *U.S. v. Torres*, No. 5:16-CR-285-DAE, 2016 WL 4821223 at *6 (W.D. Tex. Sept. 9, 2016) ("It is inappropriate for this Court to engage in a process of finesse justifying an ethereal presence of the defendant's computer in Virginia, where the plain language of the rule as now written does not provide jurisdiction under these circumstances"); *U.S. v. Croghan*, No. 1:15-CR-48, 2016 WL 4992105 at *5 (S.D. Iowa Sept. 19, 2016) (finding that the "Magistrate Judge . . . lacked authority to issue the NIT Warrant pursuant to any provision of Rule 41(b)").

B. The warrant did not and could not authorize the NIT to be installed as a tracking device.

The handful of courts that have found that Rule 41 authorized the NIT have relied on the tracking device language in section (b)(4) of the Rule. Section (b)(4) grants the magistrate judge the authority to issue a warrant to "install within the district a tracking device . . . to track the movement of persons or property" located both within the district and outside the district. Fed. R. Crim. P. 41(b)(4). A tracking device is defined for purposes of the rule at 18 U.S.C. § 3117(b) as "an *electronic or mechanical device* which permits the tracking of the movement of a person or object." Fed. R. Crim P. 41(a)(2)(E) (emphasis added). The NIT is nothing like a tracking device, and was not installed within the district.

First, the NIT does not track the target computer. Rather the NIT searches the computer for location information and other identifying information and transmits this data back to a government computer located in the Eastern District of Virginia. *See U.S. v. Croghan*, No. 1:15-CR-48, 2016 WL 4992105 at *4 (S.D. Iowa Sept. 19, 2016) (The NIT "did not 'track' the 'movement' of anything; rather, it caused computer code to be installed on the activating user's computer, which then caused such computer to relay specific information to the government-controlled computers in Virginia."); *U.S. v. Ryan Anthony Adams*, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079 at *6 (M.D. Fla. Aug. 10, 2016) ("[T]he NIT does not track; it searches"); *U.S. v. Workman*, No. 15-CV-00397-RBJ-1, 2016 WL 5791209 at *4 (D. Colo. Sept. 6, 2016) ("The government did not obtain Mr. Workman's IP address by tracking the data as it moved through various relay nodes back to Mr. Workman's computer. Rather, the government, through the NIT, searched Mr. Workman's computer and seized his IP address along with various other pieces of information.”).

Second, the NIT was “installed” on Defendant’s computer located in New York, not Virginia. Section (b)(4) specifies that, for the tracking-device warrant to be authorized, the tracking device must be installed within the district before it tracks movement outside of the district. *See U.S. v. Allain*, No. 15-CR-10251, 2016 WL 5660452, at *10–11 (D. Mass. Sept. 29, 2016) (“The NIT was downloaded from the Playpen server (located in the Eastern District of Virginia) and placed onto the ‘activating’ computers (located anywhere in the U.S.).”); *U.S. v. Henderson*, No. 15-CR-00565-WHO-1, 2016 WL 4549108, at *3–4 (N.D. Cal. Sept. 1, 2016) (pointing out that the “majority of courts have found . . . the NIT was installed on the activating computers located outside the district.”).

Third, even if the NIT could be thought of as a tracking device “installed” on the server located in the Eastern District of Virginia, “applying the tracking device exception breaks down, because [the Defendant] never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular district.” *U.S. v. Michaud*, No. 3:15-CR-05351-RJB, 2016 WL 337263 at *6 (W.D. Wash. Jan. 28, 2016); *U.S. v. Levin*, No. CR 15-10271-WGY, 2016 WL 2596010, at *6 (D. Mass. May 5, 2016) (agreeing with the reasoning in *Michaud*); *U.S. v.*

Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223 at *5 (W.D. Tex. Sept. 9, 2016) (same).

Thus the NIT warrant was not authorized by any section of Rule 41(b) and was issued in violation of the Rule insofar as it purported to authorize the search of any computer, including Mr. Palaniappan's, located outside of the Eastern District of Virginia.

III. SUPPRESSION OF EVIDENCE GATHERED AS A RESULT OF THE INTRUSION INTO MR. PALANIAPPAN'S COMPUTER IS WARRANTED.

We respectfully submit that because the initial search of Mr. Palaniappan's computer was illegal, its fruits should be suppressed. In particular, the data streams to and from Mr. Palaniappan's computer, all information identifying the computer as using Playpen, everything seized from his apartment, and his statement to the FBI during the search are all subject to suppression as fruit of the poisonous tree. *See Wong Sun v. United States*, 371 U.S. 471, 487–88 (1963). As discussed below, despite the existence of the NIT warrant, suppression is appropriate and no good-faith exception applies because (1) the warrant was not merely defective but void *ab initio*—from the beginning; (2) under controlling Second Circuit case law suppression is required where a search is justified only by a warrant signed by a judge without jurisdiction, *U.S. v. Burke*, 517 F.2d 377, 386–87 (2d Cir. 1975); (3) even if the warrant was not void, the violation of Rule 41 prejudiced Mr.

Palaniappan and was the result of the government's willful disregard of the rule. Accordingly, no good faith exception applies and the only available remedy is suppression of the unlawfully obtained evidence.

A. The NIT warrant was void *ab initio* and therefore its fruits should be suppressed.

As discussed above, the Eastern District of Virginia "lacked authority, and thus jurisdiction, to issue the NIT Warrant[.]" *U.S. v. Levin*, No. CR 15-10271-WGY, 2016 WL 2596010, at *8 (D. Mass. May 5, 2016). Accordingly, "there simply was no judicial approval." *Id. See also U.S. v. Master*, 614 F.3d 236, 241 (6th Cir. 2010) (warrant signed by judge in different county is void *ab initio*). Without a magistrate judge of competent jurisdiction issuing the warrant, the agents were not entitled to rely on the "warrant" even under the good-faith exception to the exclusionary rule. *U.S. v. Levin*, 2016 WL 2596010 at *12 (suppressing fruits of NIT warrant and observing that if the good-faith exception applied, "courts would have to tolerate evidence obtained when an officer submitted something that reasonably looked like a valid warrant application, to someone who, to the officer, appeared to have authority to approve that warrant application."); *accord U.S. v. Croghan*, No. 1:15-CR-48, 2016 WL 4992105 at *6 (S.D. Iowa Sept. 19, 2016) (good-faith exception is "inapplicable to issuance of the NIT warrant because the NIT Warrant was issued without jurisdiction and was, therefore, void *ab initio*"); *U.S. v. Workman*, No. 15-CV-00397-RBJ-1, 2016 WL 5791209, at *4 (D. Colo. Sept. 6, 2016) (suppressing NIT warrant as void *ab initio*); *U.S. v. Arterbury*, No. 15-cr-182, Clerk's No. 42 (N.D. Okla. Apr. 25, 2016) (granting motion to suppress fruits of NIT warrant).[5] Accordingly, as four district courts—*Levin*, *Croghan*, *Arterbury* and *Workman*—have already found, the warrant used to justify the search of Mr. Palaniappan's personal computer was never valid for a search outside the Eastern District of Virginia, and thus, as a matter of law, the search was warrantless, no exception to the Fourth Amendment warrant requirement applies, and the fruits of the search should be suppressed.

B. Under Second Circuit law, where a federal warrant is signed by a judge not authorized by Rule 41(b), the violation is constitutional and suppression is appropriate.

Longstanding Second Circuit case law also supports the conclusion reached by the district courts in *Levin*, *Croghan*, *Arterbury* and *Workman*. In an oft-cited case by Judge Henry Friendly, the Second Circuit made clear that where a warrant is signed by a judge without jurisdiction, suppression is warranted with no further inquiry. *U.S. v. Burke*, 517 F.2d 377 (2d Cir. 1975). In *U.S. v. Burke*, Judge Friendly addressed whether technical violations of Rule 41 were sufficient to give rise to suppression. *Id*. at 381-87.[6] In so doing, he reviewed the situation in a Fifth

[5] The *Arterbury* decision is available at https://epic.org/amicus/tracker/United-States-v-Arterbury.pdf.
[6] The specific violations of Rule 41 in *Burke* were that the warrant, on a Connecticut state form, was directed at "any Police Officer," rather than a federal agent; the warrant required execution within "a reasonable time," instead

Circuit case, *Navarro v. U.S.*, 400 F.2d 315 (5th Cir. 1968), in which the warrant application was brought to the *wrong judge*. In that situation, the Second Circuit held, the exclusionary rule should be applied for the reasons stated in *Levin*, *Croghan*, *Arterbury* and *Workman*: "While *Navarro* applied the exclusionary rule, the defect there was basic; since the issuing judge was not a 'state court of record' there was in effect no warrant at all for federal purposes." *Id*. at 386. But the circuit held that in *other* situations, exclusion is available only upon a showing of prejudice or intentional or deliberate disregard for the rule.

Judge Friendly wrote:

> [W]e think that, except in a case like *Navarro* where… the defect made what was done in effect an unconstitutional warrantless search, violations of Rule 41 alone should not lead to exclusion unless (1) there was "prejudice" in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule.
>
> *Id*. at 386-87.

In other words, under *Burke*, a Rule 41 violation alone—even without a showing of prejudice or intentional or deliberate disregard for the Rule—warrants suppression where the violation "made what was done in effect an unconstitutional warrantless search." *U.S. v. Burke*, 517 F.2d at 386–87. Although *Burke* was

---

of within ten days; and the warrant was returnable to the issuing state court, rather than to a federal magistrate. *U.S. v. Burke*, 517 F.2d at 381.

decided more than 40 years ago, it is often cited for these principles. *See*, *e.g., U.S. v. Pangburn*, 983 F.2d 449, 455 (2d Cir. 1993) (denying suppression for Rule 41 violation where officers had valid warrant but failed to provide adequate notice of search); *U.S. v. Jacobson*, 4 F.Supp.3d 515, 523 (E.D.N.Y. 2014); *U.S. v. Deas*, No. 3:07–cr–73 (CFD), 2008 WL 5063901 at *2 (D. Conn. 2008) (Droney, J.) (suppression warranted for Rule 41 violation that is "fundamental," prejudices defendant, or involves "intentional and deliberate disregard of a provision in the Rule.").

C. Suppression is warranted here because Mr. Palaniappan was prejudiced and the government willfully disregarded Rule 41.

Even if the Fourth Amendment warrant requirement had not been violated, "[i]n this Circuit, an 'intentional and deliberate disregard of a provision in the Rule,' will justify suppression[.]" *U.S. v. Turner*, 558 F.2d 46, 52 (2d Cir. 1977), *quoting U.S. v. Burke*, 517 F.2d at 386. "A showing of prejudice will also justify suppression." *Id*. Both are present here.

1. Prejudice

Judge Friendly explained in *Burke* that prejudice in this context means that "the search might not have occurred or would not have been so abrasive if the Rule had been followed." *U.S. v. Burke*, 517 F.2d at 386-87; *see also U.S. v. Krueger*, 809 F.3d 1109 (10th Cir. 2015) (finding prejudice and granting suppression where warrant issued by a Kansas magistrate judge purported to authorize a search of property already located in Oklahoma, where "the Oklahoma search might not have occurred because the government would not have obtained [the Kansas warrant] had Rule 41 been followed").

Here, two defects in the FBI's compliance with Rule 41 prejudiced Mr. Palaniappan. ***First***, the warrant was defective (if not void altogether as discussed above) because it was signed by an Eastern District of Virginia magistrate judge without power to authorize a search in New York. If the FBI had followed the rules, it would have needed a New York warrant to break into Mr. Palaniappan's personal computer. Accordingly, the search would never have taken place: the FBI did not know that Mr. Palaniappan (or anyone else) was using Playpen from the Eastern District of New York. The warrant it obtained authorized an unlawful, global fishing expedition that happened to get a bite in Queens. That would have been impossible if the rules had been followed. Therefore, "the search might not have occurred," *U.S. v. Burke*, 517 F.2d at 386, and Mr. Palaniappan was prejudiced. *See U.S. v. Levin*, 2016 WL 2596010 at *9 (finding prejudice because "had Rule 41(b) been followed, the magistrate judge would not have issued the NIT Warrant, and therefore the search conducted pursuant to that Warrant might not have occurred"); *U.S. v. Krueger*, 809 F.3d at 1116-17 (in determining whether defendant was prejudiced, the question is whether the court that issued the warrant "could have complied with the rule"). "Had Rule 41 been complied with, law enforcement would not have obtained Defendant['s] IP address[], would not have been able to link those IP address[] to Defendant[] through subsequent investigation and the use of administrative subpoenas, and would not have had sufficient probable cause to obtain the" Queens search warrant. *U.S. v Croghan,* No. 1:15-CR-48, 2016 WL 4992105 at *8 (S.D. Iowa Sept. 19, 2016).

Second, as discussed above, the government delayed notice of the search to Mr. Palaniappan until after he was arrested in violation of the plain language of the warrant and Rule 41(f)(1)(C), which requires the provision of a receipt. Fed. R. Crim. P. Rule 41(f)(1)(C). Without specifying timing, Subsection (C) required that the officer executing the warrant "give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken[.]" Fed. R. Crim. P. 41(f)(1)(C).[7] The warrant itself was more specific, stating clearly on its face that the executing officer "must give a copy of the warrant and a receipt for the property taken to the person from whom, of from whose premises, the property was taken," within 30 days.

But no one from the government notified Mr. Palaniappan or provided a copy of the warrant until more than a year later, when it was turned over in

[7] This rule was also amended, effective yesterday, to require the executing officer to make "reasonable efforts to serve a copy of the warrant and receipt on the person" searched in cases involving the remote seizure of electronically stored information. *See* Fed. R. Crim. P. 41(f)(1)(C) (2016 ed.). According to the Advisory Committee Notes, this amendment was "intended to ensure that reasonable efforts are made to provide notice of the search, seizure, or copying, as well as a receipt for any information that was seized or copied, to the person whose property was searched or who possessed the information that was seized or copied." *Id.*

discovery in the instant case. Ex. G: Gov't 4/29/16 Discovery Letter (noting that warrant was disclosed on March 16, 2016). No "receipt" was ever turned over, although a woefully inadequate "inventory" was included in the warrant return and turned over April 29, 2016. *See* Ex. H: Warrant Return. The inventory itself, rather than specify what was taken from Mr. Palaniappan, simply listed "Data from computers that accessed the TARGET WEBSITE between 2/20/15 and 3/4/15."

The failure to notify Mr. Palaniappan also prejudiced him under *Burke* because the search probably would not have taken place if the agents had to follow the rule and provide notice within 30 days. As Agent Vourderis advised Magistrate Judge Go in the Queens warrant application, secrecy was essential to the operation. "[G]iven the confidential nature of this investigation," Vourderis wrote, "disclosure would severely jeopardize the investigation in that it might alert the target(s) of the investigation at the PREMISES to the existence of an investigation and likely lead to the destruction and concealment of evidence and/or flight." Ex. B ¶ 33. If the agents had believed they were required to comply with the rule and notify the target of the search within 30 days, they probably would not have bothered. Notice would have tipped off the targets that they had identified them as Playpen user, which would, as Vourderis advises, "likely lead to destruction and concealment of evidnce," at least in the agents' minds. *Id*. Therefore, Mr. Palaniappan was prejudiced by the agents' willful failure to comply with both Rule

41(f)(1)(C) and the specific command of the NIT warrant to provide notice within 30 days.

2. “Intentional and Deliberate Disregard of the Rule”

Finally, the existing record shows that the government intentionally and deliberately disregarded Rules 41(b) and 41(f)(1)(c). In particular, the FBI obtained the NIT warrant in violation of the clear language of Rule 41(b). It made no effort to get a proper warrant in the Eastern District of New York or in the other districts where targets might be found.

Moreover, it willfully disobeyed the plain language of the warrant itself, which tracked the relevant rule, by maintaining secrecy and failing to provide notice to Mr. Palaniappan that it had searched his personal computer until long after the 30-day deadline had passed and after he had been arrested. *See U.S. v. Gantt*, 194 F.3d 987, 994–95 (9th Cir. 1999) (suppressing evidence because agents willfully disobeyed Rule 41 requirement to provide a copy of the warrant to the person searched).

The failure to comply with the warrant’s plain language is further evidence that the forum-shopping implicit in the selection of Judge Buchanan was purposeful and deliberate. To the extent the Court does not agree that the present record reveals intentional and deliberate disregard of the rule, we request a live evidentiary hearing to probe the intentions of the officers involved.

D. Suppression is appropriate in this case to deter law enforcement overreaching

Finally, we address the good-faith argument that the government is likely to interpose in opposition to this motion. Good faith, of course, does not defeat suppression here for the three reasons stated above: the search was effectively warrantless, the search would not have taken place but for the Rule 41 violations, and the government deliberately disobeyed the rules. We respectfully submit that under all these circumstances, suppression is necessary to deter law enforcement from flouting the limitations on the Rule 41 warrant authority, which strike a careful balance between law enforcement and privacy that must be respected. The decisions on which judges are authorized or whether to notify search targets are not for the FBI to make: they were made by the Supreme Court with the assent of Congress in the rule-making process. Law enforcement must be required to respect the rules as they exist, not as they wish them to be. "Exclusion of the evidence in this case will serve the remedial and prophylactic purposes of the exclusionary rule, by serving notice to the Government that use of a NIT warrant under the circumstances presented here exceeds a magistrate judge's authority[.]" *U.S. v. Arterbury*, No. 15-cr-182, Clerk's No. 42 (N.D. Okla. Apr. 25, 2016) (granting motion to suppress fruits of NIT warrant).

CONCLUSION

Because the NIT warrant was invalid and obtained and executed with willful disregard for the applicable rules, the motion to suppress should be GRANTED.

Dated: New York, New York
December 2, 2016

Respectfully submitted,
Law Office of Zachary Margulis-Ohnuma

By: /s/_________________________
Zachary Margulis-Ohnuma
Adam Elewa
260 Madison Avenue, 17th Fl.
New York, NY 10016
(212) 685-0999